IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN RE TYCO INTERNATIONAL, LTD., SECURITIES LITIGATION	02-MDL-1335-B **SECURITIES ACTION** Civil Action No. 02-1355-B

DECLARATION OF CRAIG BALL

I, CRAIG BALL, declare as follows:

Introduction

1. I am over the age of eighteen and competent to make this Declaration. I am a resident of Montgomery, Texas, and am licensed and in good standing as an attorney in the State of Texas. I have been an attorney since 1982 and am Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization. I have been admitted to practice before all Texas courts, the Fifth Circuit Court of the United States and the Federal District Courts for the Southern, Northern and Western Districts of Texas. I am familiar with the laws and rules pertaining to the discovery and production of electronic evidence in the federal system and the several states. I am widely regarded as an expert and authority in these areas and am one of only very few persons in the world to hold both a law degree and a certification in computer forensics.

Relevant Training and Experience

2. I have ceased the day-to-day practice of trial law in order to devote myself to teaching, writing and consulting, as well as serving the courts as special master and neutral expert, in the areas of computer forensics and electronic discovery. Virtually all of my

professional endeavors involve the study and practice of electronic discovery and computer forensics, a culmination of a long personal and profession interest in computers and technology.

3. I have been involved with computers since I was a child, having studied programming (BASIC) in both high school and as an undergraduate at Rice University (FORTRAN and PL/1). Beginning in the early 1980s with the advent of the personal computer, I began directing my study and experience to the integration of computing in the law office environment and, through the 1990s, to writing and lecturing across Texas and the United States about the potential of the emerging Internet as a tool in law practice and computer-aided presentation of evidence. My continuing legal education presentations about what I dubbed "Cybersleuthing," (the use of the Internet and associated databases as a tool for informal discovery), along with my web presence on the same, were the first of their kind and have been credited with introducing tens of thousands of lawyers to the power of the Internet in their practices.

4. For two years, I chaired the Technology Advisory Committee of the State Bar of Texas. In that role and working in partnership with the founders of the FindLaw website, I developed and supported a groundbreaking web portal site called MYTexasBar that currently serves more than 45,000 lawyers and their staff.

5. By virtue of my knowledge of computer operating systems, networks and applications, I am now routinely and frequently appointed as a Special Master or neutral expert by both federal and state courts. Most such appointments entail computer forensics, which is the use of specialized tools and techniques to identify, restore, analyze and present information stored on computer systems.

6. I have studied extensively in the field of computer forensics for a number of years, almost from the inception of computer forensics as a recognized discipline. I maintain an extensive library of written materials on the topic, and several of the works I have written on computer forensics have gone through peer review and/or been published in the literature of the discipline and in national publications, including TRIAL magazine, Law Technology News and publications of the American Bar Association. I am a member (by invitation) of the High Technology Crime Investigation Association and the International Information Systems Forensics Association, as well as other professional associations focused on electronic evidence. I serve as an editor of the Information Forensics Journal.

7. I am certified in Computer Forensics through a joint program of Oregon State University and New Technologies, Inc., an entity well-known for its training of FBI, NSA, IRS and CIA computer forensics experts. My training qualified for college credit and my certification entailed peer review, practical experience and two formal written examinations. Additionally, I have completed forty hours of classroom training in computer forensics by Guidance Software, Inc., the maker of the most widely used computer forensic tool in the marketplace, Encase, and another forty hours of classroom training in file system forensics and a forensics tool called WinHex. I am also formally trained in other computer forensic applications and tools and devote more than one hundred hours every year to formal classroom training on computer forensics and electronic discovery.

8. In addition to my training and experience in computer forensics, I have also devoted a large percentage of my professional study and experience to the broader discipline of electronic discovery. In that role, I have served on a number of committees and professional bodies, and I have planned and chaired several electronic evidence institutes and symposia in

Texas and throughout the United States and abroad. I testified in Washington, D.C. before the committee responsible for the amendments to the Federal Rules of Civil Procedure concerning electronic discovery. My articles on e-discovery have been published many times in the professional literature and in conjunction with continuing legal education events. I write a column devoted to electronic discovery called, "Ball in Your Court," published monthly in Law Technology News.

9. As an electronic discovery consultant, computer forensics expert or special master, I have served the courts and counsel in numerous cases, including some of the most prominent and challenging in the nation (i.e., for lead plaintiffs' counsel in the Enron/Andersen litigation and currently assisting counsel in the BP Explosion Litigation). I have also served as a consultant and instructor on computer forensics to the United States Department of Justice and as a computer forensics consultant to the State Bar of Texas' Office of Chief Counsel in disciplinary matters. Each year, I serve as an instructor in computer forensics and electronic discovery at the annual weeklong Cybercrime Summit in Kennesaw, GA. In that role, I have the privilege of teaching some of the most tech-savvy members of law enforcement and national security agencies about digital evidence. This work is supplemented by some 50+ presentations about e-discovery that I deliver to the bench and bar each year.

10. I have been engaged by the Securities Plaintiffs in the above-captioned action to address some of the difficulties and outsize costs the Securities Plaintiffs face in connection with Defendant Tyco's document production. In particular, I offer technical information and expertise to this Court in connection with its consideration of Tyco's efforts to visit the monumental costs of constructing and maintaining its unwieldy and flawed electronic discovery database on the Securities Plaintiffs. The opinions I express herein are based on my specific

knowledge and experience with respect to electronic discovery systems and methodologies as well as on information furnished to me by counsel for the Securities Plaintiffs.

Native Format Documents

11. Based on information provided to me, I understand that Securities Plaintiffs' Document Requests requested that electronic documents be produced as they are maintained in the ordinary course of business, in their native formats, and with relevant metadata (specifically file path and custodian data). I understand that Tyco has made only limited native production, electing instead to pursue poorer alternatives at greater expense.

12. Native production of electronic evidence is the superior format by any measure. It's easier to exchange and store, and less costly to produce, review, search and index. To produce one million pages electronically is trivial. If the files are email or word-processed documents, they can be recorded onto two recordable DVDs in about an hour and shipped anywhere overnight. Most importantly, native formats are the most faithful rendition of the evidence. Native production is, in both the legal and practical sense, the best evidence.

13. Tyco's concern that native production exposes them to the risk that Securities Plaintiffs will alter the native evidence and such alteration might be undetectable is unwarranted. The risk of evidence alteration has always been with us, fostered by Liquid Paper™, copying machines, scanners and printers; however, the ease with which paper can be altered never deterred its use as a production medium. In contrast to printed evidence, however, electronic evidence can in fact be made immune to undetectable alteration because simple, low- and no-cost methods exist to flush out even the tiniest alteration of electronic evidence with a level of reliability far greater than that ascribed to fingerprints and DNA tests.

14. The quick, reliable and inexpensive mechanism I reference is called "hashing," and in its most common form entails the use of a one-way cryptographic algorithm to generate a unique digital fingerprint for any item of electronic evidence, expressed as a 32-character value called a message digest. The generation of the algorithm is a routine operation, and the programs used to generate such a digital fingerprint are freely available and require no special skill to use. In fact, their use is routine among all vendors of electronic discovery services. The most common forms of hashing now in wide use is called MD5 and, though an unfamiliar name, its use lies invisibly at the heart of everyone's computer and Internet activities.

15. For example, the MD5 hash value for the full text of Lincoln's Gettysburg Address is E7753A4E97B962B36F0B2A7C0D0DB8E8. This value is calculated in a fraction of a second, and anyone, anywhere performing the same calculation on the same data will obtain the same unique value—that's the data's MD5 digital "fingerprint." Change "Four score and seven years ago" to "Five score and seven," and the hash value becomes 8A5EF7E9186DCD9CF618343ECF7BD00A. No matter how subtle the change—just omitting a period or adding a space--the hash value always changes to reflect the difference and is dramatically and detectably different from the hash value before the change.

16. In practice, Tyco can simply record the hash value for any file it produces in native format. Once these hash values are established, even the slightest alteration of the data produced would be immediately apparent because the hash value for the altered item would change in a very obvious way. It's estimated that the chance of an altered electronic document having the same MD5 hash value is one in 340 undecillion. An undecillion is a one followed by thirty-six zeros, so it's one in 340 trillion, trillion, trillion. This is a level of reliability that so far

exceeds the reliability attributed to fingerprints and DNA that it's difficult to quantify in human experience.

17. When producing original electronic evidence, Tyco converted each evidence item to a picture format called TIFF, for Tagged Image File Format. This stripped away all of the metadata associated with the original evidence and destroyed the ability to search the text of each document. Performing Optical Character Recognition ("OCR") on the images, is a poor substitute for access to the documents in their native formats.

18. Tyco converted the evidence from its files and systems, both electronic and in print, into an image format before producing it. This was a sensible step with respect to evidence existing only on paper, but an extremely poor choice for electronic documents.

The Importance Of Metadata Evidence

19. Metadata, often defined as "data about data," is evidence, typically stored electronically, that describes the characteristics, origins, usage and validity of other electronic evidence. Metadata sheds light on the context, authenticity, reliability and dissemination of electronic evidence and offers clues to human behavior.

20. There are two principal strains of metadata, which I call application metadata and system metadata. Application metadata is information typically absent from the printed page and embedded in the file it describes, moving with the electronic file when you copy it to a new location, e.g., to a floppy disk or to another computer. By contrast, system metadata is not embedded in the file it describes, but is stored externally and used by the computer's file system to track file locations and store demographics. Because it's not a part of the file, it is left behind when the file is moved to a new container (e.g., to a CD or another hard drive), or when it's transmitted to another system (e.g., over a network or via e-mail). A file's name, size, location,

path and dates of creation, modification and access are common system metadata fields, but there are many others. Not all metadata is embedded for the same reason that cards in a library card catalog aren't stored between the pages of the books. Having both embedded application metadata and external system metadata is advantageous because, when metadata is stored both within and without a file, discrepancies between the metadata can expose data tampering. Metadata thus serves a key role in the authentication of evidence.

21. The most important feature of metadata is that it enables one to sort and categorize electronic evidence. Without metadata, it's difficult and sometimes impossible to ascertain when a document was created, modified or accessed, or to determine its author or custodian. An electronic filing system stripped of metadata is like a gigantic file room where none of the file cabinets, drawers or folders are labeled.

22. Metadata is both evidence and a key to validating and understanding other evidence. Because application metadata is part of the file, litigants are obliged to preserve it and, when requested and relevant, to produce it commensurate with their obligation to preserve and produce, e.g., marginalia on paper documents. System metadata is akin to the manila folders, labels, pagination and even staples that helped make sense of pre-digital production and therefore is an integral part of a litigant's production duty. Since a digital document's system metadata is stored outside the file, it doesn't move with the file, so it must be preserved or "captured" in some manner. This may be done by manually recording the values or by printing the metadata to a slip-sheet, but it's customarily accomplished automatically by exporting metadata to a spreadsheet, database or load file.

Searchability of Images and Text

23. When electronic evidence is stored on a computer in its native format (e.g., as a Microsoft Word document, an Excel spreadsheet or an e-mail), the text it contains is

electronically searchable—an essential characteristic when the volume of information grows far beyond that which a person can practically search by reading every page. However, when an electronic document becomes a TIFF image file—a picture of the evidence—it loses its ability to be searched electronically. To offset this loss of searchability, either the textual content of the evidence must be carried over ("piped" or "exported") from the original, or something must read the picture and retype the text. The first approach is by far the most desirable because, by pulling text directly from the original without the necessity of interpretation, the exported text is 'perfect'—that is, it faithfully reflects the text of the original. Moreover, exporting the text is instantaneous and occasions little or no cost. It is, in summary, the best practice to follow in conjunction with conversion of electronic documents to image formats.

Recommended Action

24. Evidence maintained in the ordinary course of business, that is, in its native electronic format along with relevant and accessible system metadata, is no more than the evidence's original and unabridged format. It is the format that most easily affords the plaintiffs a level of access to the evidence in the case on par with that currently enjoyed by the defendant. The evidence's metadata sheds light on the evidence's origins and authenticity. Without this metadata--information that is readily available to Tyco and used in its day-to-day operations--Securities Plaintiffs won't have a commensurate ability to access, sort, search, manage and authenticate the evidence. As discussed, the Tyco production process largely strips this important evidence away, just as if Tyco had redacted all dates and notarial acknowledgements from paper documents before producing them. Tyco chose a system that stripped such data despite Securities Plaintiffs' express request for the data in its native format with metadata.

25. By far, the least costly way to transfer electronic evidence is electronically, in its native format. Because this is the format in which the information resides on Tyco's own systems and servers, native production requires no conversion and no processing beyond that which is required to move it from one medium to another. Native formats require no optical character recognition to extract electronically searchable text because such text as may exist is already in an electronic form and often searchable.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: March 30, 2006

Craig Ball